IN THE CLAIMS

In response to the Examiner's Amendment in the Notice of Allowance mailed 01/22/2008, please amend the claims as follows:

1. (Previously Presented) A method executed utilizing a computer including a tangible computer readable medium for prioritized network security, comprising:
identifying a set of policies, each policy having a condition associated therewith;
determining whether the conditions are met;
determining whether a user confirms activation of the policies; and
activating the policies whose associated conditions are determined to be met if the user confirms the activation;
wherein the conditions are based on a priority of the policy;
wherein a first policy with a higher priority has a first condition associated therewith that is different from a second condition associated with a second policy with a lower priority such that the first policy and second policy are activated under different priority-related conditions;
wherein the activation of the policies includes:

adding the policies to a set of a plurality of active policies, and executing security actions associated with the active policies if associated limits are met; and

identifying currently executed security actions, determining whether a conflict exists between the currently executed security actions, and resolving any conflicts between the currently executed security actions;
wherein the conditions are based on a time factor, the time factor including at least one of a timeframe, a predetermined time period, and a time limit;
wherein the conditions are based on a source of the policies;
wherein the conditions are based on a severity of security actions associated with the policies.

2. (Cancelled)

3. (Cancelled)

4. (Original) The method as recited in claim 1, and further comprising updating the set of policies.

5. (Original) The method as recited in claim 4, wherein the updating includes receiving another inactive policy, determining whether the user accepts the inactive policy, and adding the inactive policy to the set if the user accepts the inactive policy.

6. (Cancelled)

7. (Previously Presented) The method as recited in claim 1, and further comprising determining whether the conditions associated with the active policies are still met, and de-activating the active policies if the associated conditions are not met.

8. (Cancelled)

9. (Cancelled)

10. (Cancelled)

11. (Cancelled)

12. (Previously Presented) A computer program product embodied on a tangible computer readable medium for prioritized network security, comprising:
computer code for identifying a set of policies, each policy having a condition associated therewith;
computer code for determining whether the conditions are met;

computer code for determining whether a user confirms activation of the policies; and

computer code for activating the policies whose associated conditions are determined to be met if the user confirms the activation;

wherein the conditions are based on a priority of the policy;

wherein a first policy with a higher priority has a first condition associated therewith that is different from a second condition associated with a second policy with a lower priority such that the first policy and second policy are activated under different priority-related conditions;

wherein the activation of the policies involves:

computer code for adding the policies to a set of a plurality of active policies, and executing security actions associated with the active policies if associated limits are met; and

computer code for identifying currently executed security actions, determining whether a conflict exists between the currently executed security actions, and resolving any conflicts between the currently executed security actions;

wherein the conditions are based on a time factor, the time factor including at least one of a timeframe, a predetermined time period, and a time limit;

wherein the conditions are based on a source of the policies;

wherein the conditions are based on a severity of security actions associated with the policies.

13. (Cancelled)

14. (Cancelled)

15. (Original) The computer program product as recited in claim 12, and further comprising computer code for updating the set of policies.

16. (Original) The computer program product as recited in claim 15, wherein the updating includes receiving another inactive policy, determining whether the user accepts the inactive policy, and adding the inactive policy to the set if the user accepts the inactive policy.

17. (Cancelled)

18. (Previously Presented) The computer program product as recited in claim 12, and further comprising computer code for determining whether the conditions associated with the active policies are still met, and de-activating the active policies if the associated conditions are not met.

19. (Cancelled)

20. (Cancelled)

21. (Cancelled)

22. (Cancelled)

23. (Currently Amended) A system including a computer with a tangible computer readable medium for prioritized network security, the medium comprising:
logic for identifying a set of policies, each policy having a condition associated therewith;
logic for determining whether a user confirms activation of the policies;
logic for determining whether the conditions are met if the user confirms the activation; and
logic for activating the policies whose associated conditions are determined to be met;
wherein the conditions are based on a priority of the policy;

wherein a first policy with a higher priority has a first condition associated therewith that is different from a second condition associated with a second policy with a lower priority such that the first policy and second policy are activated under different priority-related conditions[[:]];
wherein the activation of the policies involves:

logic for adding the policies to a set of a plurality of active policies, and executing security actions associated with the active policies if associated limits are met; and

logic for identifying currently executed security actions, determining whether a conflict exists between the currently executed security actions, and resolving any conflicts between the currently executed security actions;
wherein the conditions are based on a time factor, the time factor including at least one of a timeframe, a predetermined time period, and a time limit;
wherein the conditions are based on a source of the policies;
wherein the conditions are based on a severity of security actions associated with the policies.

24. (Cancelled)

25. (Cancelled)

26. (Cancelled)

27. (Cancelled)

28. (Previously Presented) A method executed utilizing a computer including a tangible computer readable medium for prioritized network security, comprising:
identifying a set of policies, each policy having a condition associated therewith;
determining whether a user confirms activation of the policies;
determining whether the conditions are met; and

activating the policies whose associated conditions are determined to be met if the user confirms the activation;
wherein the conditions are based on an urgency associated with an issue causing the policy to be activated;
wherein a first policy with a higher associated urgency has a first condition associated therewith that is different from a second condition associated with a second policy with a lower associated urgency such that the first policy and the second policy are activated under different urgency-related conditions;
wherein the activation of the policies includes:

adding the policies to a set of a plurality of active policies, and executing security actions associated with the active policies if associated limits are met; and

identifying currently executed security actions, determining whether a conflict exists between the currently executed security actions, and resolving any conflicts between the currently executed security actions;
wherein the conditions are based on a time factor, the time factor including at least one of a timeframe, a predetermined time period, and a time limit;
wherein the conditions are based on a source of the policies;
wherein the conditions are based on a severity of security actions associated with the policies.

29. (Previously Presented) A method executed utilizing a computer including a tangible computer readable medium for providing network security, comprising:
identifying a set of a plurality of inactive policies each including a security action, a condition for activating the policy, and a limit for triggering the security action if the policy is active;
updating the set of inactive policies including:

receiving another inactive policy,

determining whether a user accepts the inactive policy, and

adding the inactive policy to the set if the user accepts the inactive policy;

determining whether the conditions are met for the inactive policies;

determining whether the user confirms the activation of the inactive policies if the associated conditions are met; and

activating the inactive policies if the user confirms, the activation including:

adding the inactive policies to a set of a plurality of active policies,

determining whether the conditions associated with the active policies are still met,

de-activating the active policies if the associated conditions are not met, and

executing the security actions associated with the active policies if the associated conditions are met and the limits are met, the execution of the security actions including:

identifying currently executed security actions,

determining whether a conflict exists between the currently executed security actions, and

resolving any conflicts between the currently executed security actions;

wherein the conditions are based on a time factor, the time factor including at least one of a timeframe, a predetermined time period, and a time limit;

wherein the conditions are based on a source of the policies;

wherein the conditions are based on a severity of security actions associated with the policies.

30. (Previously Presented) The method as recited in claim 1, wherein the policies include low priority policies that are default policies which do not expire.

31. (Previously Presented) The method as recited in claim 1, wherein the policies include medium priority policies that are valid for the predetermined time period.

32. (Previously Presented) The method as recited in claim 31, wherein the policies include high priority policies that are valid for another predetermined time period that is less than the predetermined time period associated with the medium priority policies.

33. (Previously Presented) The method as recited in claim 1, wherein the identifying the set of policies, the determining whether the conditions are met, and the activating the policies are controlled locally.

34. (Previously Presented) The method as recited in claim 1, wherein the associated conditions of the policies dictate the manner in which the active policies are to be deactivated.

35. (Previously Presented) The method as recited in claim 1, and further comprising determining whether one of the active policies is still active including determining whether the condition associated with the active policy is still met.

36. (Previously Presented) The method as recited in claim 35, and further comprising de-activating the active policy if the associated condition is not met and determining whether the de-activated policy is to be reused or discarded.

37. (Previously Presented) The method as recited in claim 36, wherein an indication of the determination whether the de-activated policy is to be reused or discarded is stored with the associated condition.

38. (Previously Presented) The method as recited in claim 1, wherein the conditions are based on the detection of a predetermined amount of files of a certain type.

39. (Previously Presented) The method as recited in claim 1, wherein the conditions are based on whether a virus signature update is current.